

"La gestión de vulnerabilidades será una commodity dentro de la seguridad"

(Qualys)

Más conocida por su oferta para la gestión de vulnerabilidades, la gran baza de Qualys es identificar los activos de las empresas, recopilar y analizar datos de seguridad de TI, descubrir y priorizar vulnerabilidades, recomendar acciones de remediación y verificar la implementación de dichas acciones. Una gran tarea en los entornos descentralizados de las TI, y cuando hay que hacer frente al cloud, al shadow IT o al IoT.

Proveedor de seguridad cloud y de soluciones de cumplimiento, Qualys facturó 278,9 millones de dólares en 2018, un 21% más respecto al año anterior, con un beneficio neto de 53,7 millones de dólares. Tiene una capitalización de mercado de 3.400 millones de dólares y durante este año tiene previsto crecer entre un 15% y un 16%, hasta los 323 millones de dólares. Según IDC es uno de los líderes del mercado de gestión de vulnerabilidades, con la quinta mayor cuota de este mercado, valorado por la consultora en 6.700 millones de dólares.

Pero hay mucho más. A través de su Qualys Cloud Suite la compañía ofrece no sólo soluciones





"Es esencial hablar de visibilidad antes de hablar de seguridad o de vulnerabilidades"

de gestión de vulnerabilidades, sino de monitorización continua, Cloud Agent, AssetView, ThreatPROTECT, Cumplimiento de políticas, Cumplimiento PCI, Escaneo de aplicaciones web y WAF (Web Application Firewall). El objetivo de todo ello es ayudar a los clientes a conseguir la visibilidad de sus activos de TI; nos lo ha contado Raúl Benito, el responsable de Qualys para el mercado de Iberia.

Fundada en 1999 en California, la compañía acumula más de 10.000 clientes en más de 130 países, incluido el Banco de Santander desde finales de 2018, un año marcado por tres adquisiciones: 1Mobility en abril, Second Front System en junio y Layered Insight en octubre. No suma muchas más esta empresa. La primera compra fua de la NetWatcher, una compañía de seguridad de red, en diciembre de 2017, y la última ha sido la de Adya el pasado mes de febrero.

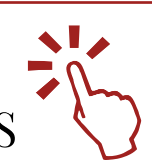
Qualys ha evolucionado al ritmo del propio mercado, un mercado en el que la demanda de soluciones de ciberseguridad sigue en alza, en el que el coste de un ciberataque puede alcanzar el trillón de dólares e impactar en millones de usuarios. Un mercado en el que las empresas se han dado cuenta de la necesidad de contar con medidas de seguridad más estrictas. Un mercado en el que la transformación digital, la adopción del cloud y la proliferación de dispositivos conectados exponen a las empresas desde el punto de vista de la seguridad.

Qualys evoluciona al ritmo del mercado y por eso a finales del año pasado lanzaba la solución Qualys Container Security para mejorar la seguridad y visibilidad de las aplicaciones en contenedores que se ejecuten en Amazon Web Services "en sólo unos pocos clicks". Y con este mismo proveedor de cloud, concretamente con AWS Security Hub, anunciaba esta compañía una integración con la que poder aplicar cumplimiento de políticas y vulnerabilidades que permitan a los clientes priorizar los riesgos y automatizar la remediación utilizando servicios nativos, como AWS Lambda.

Costó mucho avanzar porque en el momento de la fundación de la compañía "hablar de cloud era complicado", tanto "como encontrar ingenieros en Silicon Valley", explica Raúl Benito. Por eso la compañía estableció en Pune, India, un departamento de desarrollo, con ingenieros altamente cualificados. El tiempo fue pasando y es ahora cuando "la explosión de la gestión de vulnerabilidades está llegando" asegura el responsable de la compañía en la región de Iberia, añadiendo que



LA GESTIÓN DE VULNERABILIDADES



Es imperativo para cualquier organización implementar una Gestión de Vulnerabilidades efectiva para protegerse contra ataques y amenazas. El panorama de amenazas de hoy es inimaginablemente diferente, con miles de nuevas vulnerabilidades reportadas cada año y la creciente complejidad del entorno de la organización. Diferentes informes sobre brechas de seguridad muestran un claro aumento en el número de vulnerabilidades identificadas y la forma de explotarlas.



El gran volumen de ataques exige las mejores soluciones de administración de vulnerabilidades en su clase que ofrecen un descubrimiento completo para respaldar todo el ciclo de vida de la administración de vulnerabilidades.

eso es tanto por la madurez del mercado como de las herramientas; "el momento es bueno en cuanto a que el comité de dirección de las empresas tiene conciencia de que la seguridad es importante para la continuidad de negocio, y la parte de gestión de vulnerabilidad es esencial a la hora de poder medir el riesgo que pueda tener tu empresa".

Pero más que la propia vulnerabilidad en sí, asegura Raúl Benito que lo esencial es la visibilidad. La visibilidad de los activos es la clave de las adquisiciones que se han realizado en los últimos años, dice el directivo. ¿Y qué es un activo? "Cualquier cosa que pueda tener valor dentro de tu empresa y que se pueda conectar a tu red. Hablamos de móviles, hablamos de cámaras, hasta un termostato, y por supuesto los laptops, PCs y servidores", dice Benito recalcando que para la compañía "es esencial hablar de visibilidad antes de hablar de seguridad o de vulnerabilidades" y que por eso "es muy importante todas las integraciones que empezamos a tener con el mundo CMDB (Configuration Management Database)".

Aquí entra en juego la importancia del activo, porque no es lo mismo uno que tenga una vulnerabilidad crítica si en él se sustenta parte de tu negocio esencial, a si es un activo que está sustentando algo que es totalmente prescindible. Esa visibilidad es importante cuando se habla de vulnerabilidades porque "te ayudar a saber en qué activos tienen que actuar cuanto antes y de qué forma; y en algunos será parcheando y en otros lanzando un mensaje al IPS, al firewall o al EDR

> Visibilidad y gestión de vulnerabilidades parece el cóctel perfecto para hacer frente al fascinante, y peligroso, mundo del Internet de las Cosas



para que toma ciertas acciones que impidan que se explote la vulnerabilidad".

Esta es en opinión de Raúl Benito, la esencia de Qualys: darte una visibilidad y una seguridad que puedas consumir. Lo que a su vez está alienado al

"Ya no es la virtualización, ahora son los contenedores y los microservicios, y para nosotros es vital tener visibilidad"

foco que tiene Qualys en la integración con terceros vía API o vía conectores, algo que se tiene con los principales SIEM del mercado, con los PAMs en términos de autenticación, con los IPS…, "para poder darte una información que tú puedas utilizar", poderle decir al resto de herramientas lo que se tiene que hacer para que una vulnerabilidad no sea explotable.

Cloud, IoT, Contenedores

Sobre el cloud dice el directivo que es una tendencia a la que las empresas no podrán resistir mucho tiempo, "de forma que cuanta mayor visibilidad tengas de esos entornos que no controlas mucho mejor". ¿Os acerca esto al mundo de los CASB (Cloud Access Security Broker)? "No, porque nosotros no vamos a evaluar la seguridad en la comunicación o en el servicio, sino evaluar la seguridad de tus activos propiamente dicho, cómo tú los has definido". Y añade Raúl Benito que las empresas que nacen en la nube entienden que todo sus servicios están parcheados a lo último; "se tiene todo en la nube, todo se actualiza cuando se tiene que actualizar y los negocios se adaptan. Los PCS son terminales tontos que se conectan y trabajan en aplicaciones, y aunque ahora este concepto suene muy avanzado para muchas empresas, es donde terminaremos".

Visibilidad y gestión de vulnerabilidades parece el cóctel perfecto para hacer frente al fascinante, y peligroso, mundo del Internet de las Cosas. "En IoT no me hables de parchear", dice Raúl Benito. La mayoría de las veces porque no se puede, pero lo que parece imprescindible es tener visibilidad de lo que se está haciendo.

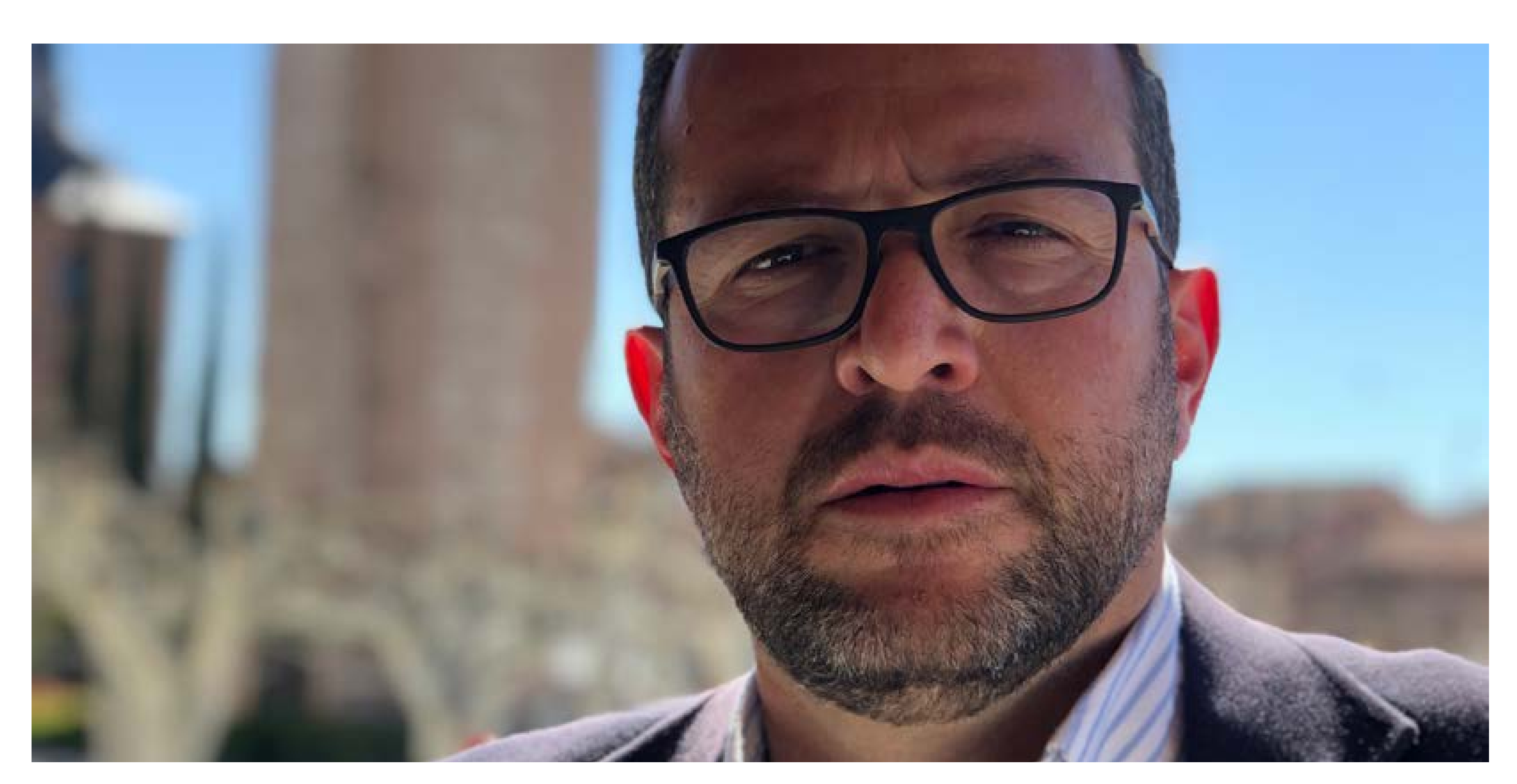
"Nosotros tenemos una capacidad de poder escanear la red de forma masiva de una manera muy eficiente para que no repercuta en el trabajo o en el negocio del cliente", dice el ejecutivo de Qualys. La categorización que hace la compañía permite

establecer el tipo de aplicativo y el tipo de acción que realiza, y "esa homogenización o estandarización de todo lo que se encuentre es esencial para poder empezar a tomar decisiones".

Sobre los contenedores, quizá el mercado no preveía que su crecimiento iba a ser tan exponencial. Han revolucionado el mundo de las TI; "va a cambiarlo todo, ya no es la virtualización, ahora son los contenedores y los microservicios, ya no necesito construir mi sistema operativo virtualizado, y para nosotros es vital tener visibilidad de lo que se está construyendo porque la flexibilidad y elasticidad que tienen estas nuevas tecnologías es increíble".

Explica Raúl Benito que Qualys se integra en la tecnología de contenedores para que se pueda tener visibilidad de lo que se está construyendo en cuanto a seguridad, pero además "permite que pongas tus propias políticas de compliance en función a la seguridad que tú estás metiendo en ese microservicio".

Planteamos al responsable de Qualys para la región de Iberia que llevando como llevamos tanto tiempo hablando de BYOD y de Shadow IT, la visibilidad debería ya darse por hecha. "Claro, pero al final seguimos hablando de silos", ahora por fin la gente de seguridad tiene un nivel de interlocución alto dentro de las empresas que hace que la seguridad empiece a ser transversal a cualquier cosa que se haga en la empresa, y eso hace que tanto el BYOD como la parte móvil, la parte de IoT o la parte Cloud "tendrá que ser compliance con normativa que yo tengo de seguridad en mi empresa".



"La solución de Qualys es tan buena o tan mala como las manos que la estén implementando, y por eso se está invirtiendo mucho en formación para el canal"

Qualys Iberia

Qualys arranca en Iberia con personal propio hace dos años. Se ficha Raúl Benito, un veterano con experiencia en Trend Micro, Check Point o McAfee. Hace un año se incorporó Sergio Pedroche, con más de diez años de experiencia en el mundo de la ciberseguridad. Nos cuenta Benito que ahora se incorpora otra persona, y otra más a mitad de año,

Fundada en 1999 en California, la compañía acumula más de 10.000 clientes en más de 130 países, incluido el Banco de Santander desde finales de 2018



lo que demuestra la inversión local que está haciendo la compañía.

Dice el directivo que "la solución de Qualys es tan buena o tan mala como las manos que la estén implementando, y por eso se está invirtiendo mucho en formación para el canal".

De momento no se trabaja con mayorista, y sí y mucho con canal especialista. "Trabajamos mucho con los principales SOC que pueden existir en el mercado, como los S21Sec, Aiuken, Satec, BT…", explica Raúl Benito, añadiendo: "para nosotros la gestión de vulnerabilidades será una commodity dentro de la seguridad. A lo mejor no escaneas todos los días todos los activos, porque no es necesario. Lo que no puede ser es que una empresa no sepa cuántos activos tiene y qué riesgo pueden tener; y con herramientas como la nuestra, con un despliegue muy sencillo pueden tener esa visibilidad".

Enlaces de interés…

- Qualys Patch Management para el parcheado automático de aplicaciones
- Qualys AI ayuda a los equipos de seguridad a identificar riesgos
- Qualys compra activos de Adya para potenciar la gestión de aplicaciones cloud
- Qualys quiere extender su presencia en departamentos gubernamentales con una compra
- Qualys refuerza sus capacidades móviles con la compra de 1Mobility
- Qualys adquirirá los activos de NetWatcher

Compartir en RRSS

